DATE: 3 JULY 2023

Supervisory benchmark No 1/2023

On client due diligence via the transaction monitoring system

The Czech National Bank (hereinafter the "CNB") carries out, *inter alia*, control activities for of prevention of money laundering and terrorist financing with respect to the obliged entities over which it exercises supervision. This benchmark primarily applies to credit institutions - banks (hereinafter "obliged entities" or "banks"), however it can be appropriately and adequately applied to other financial market entities in proportion to their size and the structure of products and services they provide.

Content of the supervision benchmark:

Relevant legislation **2**

Purpose and general assumptions **3**

I. Assumptions of the regulatory base and risk-based approach **4**

i. Risk-Based Approach 5

ii. System of internal rules and risk assessment 5

II. Prerequisites for effective and adequate AML transaction monitoring **6**

i. Data and detection scenarios 6

ii. Internal transfers between accounts of the same client or between clients within the framework of a given obliged entity 7

iii. Non-bank financial institutions in the position of a client of an obliged entity 8

iv. Investment instruments 9

v. IS/IT prerequisites 11

III. Prerequisites for the process procedures area **12**

i. Timeframes for alert generation and investigation 12

ii. Procedures for alert investigation, whitelisting 14

iii. Alert closure 15

IV. AML monitoring using artificial intelligence (AI) **16**

Conclusion **17**

Annex 1 - Selected parts of MiFID II requirements for the purpose of: (i) product governance and (ii) suitability assessment **18**

Relevant legislation

Key regulations and selected provisions

- Act No 253/2008 Coll., on selected measures against legitimisation of proceeds of crime and terrorist financing, as amended (hereinafter the “AML Act”)
  - in particular Article 9, Article 9a, Article 15, Article 18(1), Article 21(1), Article 21a
- Decree No 67/2018, on selected requirements for the system of internal rules, procedures and control measures against legitimisation of proceeds of crime and terrorist financing, as amended by Decree No 253/2021 Coll. (hereinafter the "AML Decree")
  - in particular Article 8(1), Article 9(2)(a), Article 17(2), Article 17a, Article 18
- Decree No 163/2014 Coll., on the performance of the activities of banks, credit unions and investment firms, as amended (hereinafter “Decree No 163/2014 Coll.”)
- Act No 69/2006 Coll., on the implementation of international sanctions, as amended, and related legislation in the form of sanctions established by directly applicable European Union (hereinafter "EU") legislation issued by the relevant EU bodies and published in the Official Journal of the EU, and the relevant interpretative opinions of the European Commission on these regulations[1]
- Act No 1/2023 Coll., on restrictive measures against certain serious acts in international relations (hereinafter the “Sanctions Act”)

Selected methodological guidelines, risk assessments and recognised AML/CFT standards

- Basel Committee on Banking Supervision: Guidelines – Sound management of risks related to money laundering and terrorist financing
- FATF – Risk-based Approach Guidance for the Securities Sector
- EBA/GL/2021/02 - The Guidelines on client due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (‘The ML/TF Risk Factors Guidelines’) pursuant to Articles 17 and 18(4) of Directive (EU) 2015/849), repealing and replacing Guidelines JC/2017/37 (hereinafter “EBA/GL/2021/02”)
- EBA/GL/2019/04 - EBA Guidelines on ICT and security risk management
- EBA/GL/2019/02 - EBA Guidelines on outsourcing
- CNB Communication on the EBA Guidelines on outsourcing[2]
- Financial Analytical Office (hereinafter the "FAO") - Report on the second round of the national money laundering and terrorist financing risk assessment process[3]

[1] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/restrictive-measures-sanctions_en.

[2] https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/obecne-pokyny-evropskych-organu-dohledu/Sdeleni-CNB-o-obecnych-pokynech-EBA-k-outsourcingu/.

[3] The aim of the national risk assessment (hereinafter “NRA”) process is to assess the risks of money laundering and terrorist financing in the Czech Republic in cooperation with all stakeholders and to prepare a report on this. The process is coordinated by the FAO and governed by the relevant Financial Action Task Force (hereinafter “FATF”) methodology, the fifth AML Directive and the AML Act. The current public version is published on the website: https://www.financnianalytickyurad.cz/narodni-hodnoceni-rizik.

Purpose and general assumptions

This supervision benchmark responds to selected, in particular recurring, control findings in the system of preventive measures an obliged entity must apply in order to effectively implement procedures to conduct ongoing client due diligence through regular monitoring of transactions[4] (hereinafter "AML monitoring").

AML monitoring is an integral part of a comprehensive system of prerequisites and measures in the fight against money laundering and terrorist financing, and synergistically complements other measures, such as the client identification and due diligence obligation[5], regular training, archiving, reconstructability of processes, etc. In addition to the above, the system is also made up of interlinkages between other necessary measures (in particular the calculation of the riskiness of the client/products or transactions[6], checks relating to international sanctions), and therefore AML monitoring assumes their interconnection. Establishing, linking and applying these related measures is key to detecting and investigating suspicious transactions.

The warnings in the text target in particular the following areas:

- **Regulatory base**
  This chapter primarily highlights weaknesses in the system of internal rules and the risk-based approach. It also includes notes on the methodologies governing implementation practice.

- **AML transaction monitoring performance and technical prerequisites**
  This chapter deals with the actual setup of AML monitoring and, *inter alia*, emphasizes a properly technically set up and functioning AML monitoring system as a prerequisite for the overall eligibility of the management and control system (hereinafter the "MCS").[7] In view of this, there is a strong interdependence with requirements arising from the area of information systems/information technology (hereinafter “IS/IT”) supervision. The IS/IT requirements therefore synergistically complement the demands placed on AML monitoring.[8]

- **Process procedures**
  The focus of the chapter is on workflows for assessing the risk of suspicious transactions, including downstream processes. In the context of AML monitoring, obliged entities usually use semi-automated solutions, either commercially available or developed in-house. In the event the parametric conditions given by the individual detection scenarios are met, alerts are generated and subsequently investigated by the relevant employees of the obliged entity (or persons involved in the activities of the obliged entity through outsourcing)

[4] For the purposes of this document, the term "transaction" is used in the sense of "any interaction" as defined in Article 4(1) of the AML Act. The term "transaction" is used in practice in the context of AML monitoring at credit and financial institutions, and in particular banks, and is therefore also introduced in this document.

[5] Client due diligence in the broader sense, i.e. including in relevant cases ascertaining the ownership and management structure of the client, ascertaining the identity of the beneficial owner, etc.

[6] Whether this involves an individual or a sequence/set of interdependent transactions in the context of the situation (e.g. client behaviour, business case structure, transaction structuring, etc.).

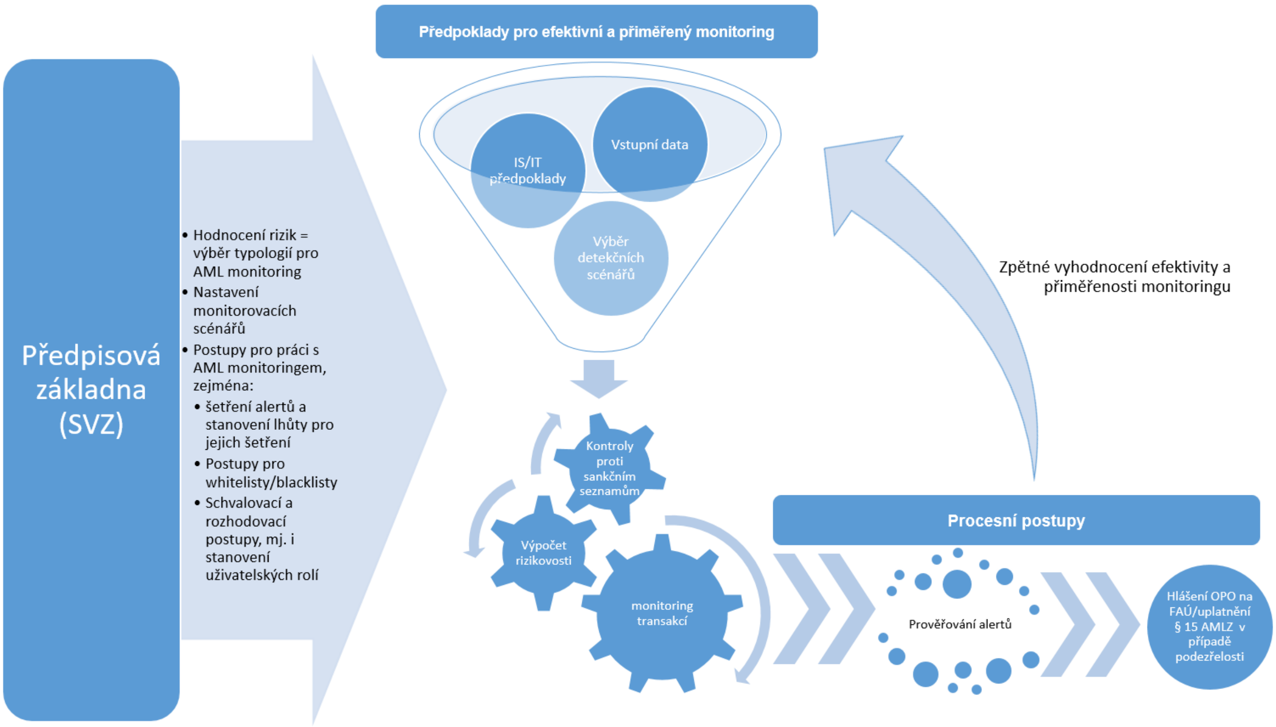
[7] MCS in the meaning of Decree No 163/2014 Coll.

[8] This chapter is therefore intended for AML/compliance officers as a benchmark for what should be set (should be required) in regard to an obliged entity by the departments in charge of IS/IT issues.

responsible for the prevention of money laundering and terrorist financing (hereinafter "AML") agenda.

- **New trends**
  Highlighting areas where specific risks need to be assessed with regard to the use of new technologies, in particular using artificial intelligence (hereinafter “AI”) elements.

The overall concept of AML monitoring can be simplified as follows:


Předpoklady pro efektivní a přiměřený monitoring
IS/IT předpoklady
Vstupní data
Výběr detekčních scénářů
Předpisová základna (SVZ)
• Hodnocení rizik = výběr typologií pro AML monitoring
• Nastavení monitorovacích scénářů
• Postupy pro práci s AML monitoringem, zejména:
• šetření alertů a stanovení lhůty pro jejich šetření
• Postupy pro whitelisty/blacklisty
• Schvalovací a rozhodovací postupy, mj. i stanovení uživatelských rolí
Kontroly proti sankčním seznamům
Výpočet rizikovosti
monitoring transakcí
Zpětné vyhodnocení efektivity a přiměřenosti monitoringu
Procesní postupy
Prověřování alertů
Hlášení OPO na FAÚ/uplatnění § 15 AMLZ v případě podezřelosti

I. Assumptions of the regulatory base and risk-based approach

In conjunction with the AML Decree, the AML Act explicitly imposes the obligation to monitor transactions and regulates certain other aspects of AML monitoring. The main pillar of this obligation is Article 9(2)(d) of the AML Act[9], which provides for the obligation to monitor the business relationship and transactions carried out in the course of that relationship on an ongoing basis. Ongoing monitoring of the business relationship and individual transactions must be carried out to the extent necessary to assess the risk of money laundering and terrorist financing (hereinafter "ML/TF")[10]. Article 21(5) of the AML Act further requires an obliged entity sets up procedures for conducting client due diligence appropriate to the ML/TF risk, according to the type of client, product, etc.

[9] Also Article 9a(3)(c) of the AML Act, see the chapter Risk-Based Approach for more details.

[10] Article 9(3) of the AML Act.

i. Risk-Based Approach

In its totality, the AML legislation forms the basis for the mandatory application of the so-called Risk-Based Approach (RBA). An RBA, as defined in particular pursuant to Article 21(5) of the AML Act (in particular (d)) and Article 5 of the AML Decree, requires obliged entities to take appropriate steps to identify and assess the ML/TF risk, taking into account risk factors relating to their customers, country/countries of origin, products, services, transactions and supply channels. These steps should be directly proportional to the nature and size of the obliged entity. In relation to the identified risks, obliged entities must have processes, control mechanisms and procedures in place to manage or effectively control ML/TF risks identified at EU level, national risk assessment level, and through risk assessment of the obliged entity.

The AML Decree provides in Article 8(1) that the measures contained in the obliged entity's internal system must be set up in such a way as to ensure, *inter alia*, that the obliged entity is able to effectively manage risks and identify any suspicious transactions. As part of such measures, the obliged entity is to establish and apply procedures including the scope and frequency of the client due diligence measures carried out[11]. For customers with increased risk pursuant to the RBA, Article 9a(3)(c) of the AML Act and Article 9(2)(a) of the AML Decree require enhanced monitoring of the business relationship and transactions within it. Enhanced monitoring can then generally be understood as more frequent monitoring of transactions by a risky entity and lower preset limits.

In view of the above, the CNB considers the following approaches, for example, to be insufficiently prudent:

- **The risk-based approach is not continuously adapted to the changing conditions of the product, client and transaction portfolio or distribution channels, i.e. in general to situations which are in particular part of the system of internal rules** (hereinafter the "SIR" or "regulatory base"[12]) **and the risk assessment for the obliged entity, as a result of which the obliged entity is, *inter alia*, exposed to the risk of violating Article 4(4), (5) and (7) of the AML Decree.**

ii. System of internal rules and risk assessment

The obliged entity will prepare the SIR pursuant to Article 21 of the AML Act. The **SIR is a comprehensive document bringing together the procedures and measures of an obliged entity** to the extent that it carries out activities subject to the AML Act **prepared on the basis of a risk assessment.[13]**

The obligation to implement appropriate systematic measures within the SIR can also be derived from the AML Decree. The AML Decree further provides that such measures must also be retroactively reconstructable[14]. The requirement of reconstructability is contained in Article 16(3)

[11] Article 8(2)(b) of the AML Decree.

[12] This benchmark uses the term "system of internal rules" within the meaning of the AML Act (Article 21(2)) and the AML Decree (Article 4). The system of internal rules is a comprehensive system of all regulations, procedures, internal controls, methodological instructions, processes and system measures that the obliged entity has set up for the purpose of combating money laundering and terrorist financing.

[13] Article 21a of the AML Act.

[14] Article 18(1) of the AML Decree.

of the AML Act and further elaborated in Article 18(2) of the AML Decree. Together, these provisions impose the obligation to properly document the business relationship and individual transactions in a manner and to an extent that ensures they are sufficiently probative. One of such measures to be adopted by the obliged entity is the internal methodology for AML monitoring, which is part of the obliged entity's SIR and which it further appropriately complements.[15]

In view of the above, the CNB considers the following approach by an obliged entity, for example, to be insufficiently prudent:

- **When it inadequately develops its regulatory base, which does not establish working/methodological procedures for AML monitoring, such as procedures for:**
    - **evaluating scenarios to detect suspicious transactions,**
    - **setting the detection limits, or "thresholds"[16],**
    - **updating parametric lists (list of countries, products, payment codes, etc.),**
    - **verifying the data record decisive for the alert calculation (i.e. whether the data for the computational model are complete, correct and up-to-date),**
    - **alert investigation (including prioritization, which governs the processing of multiple alerts),**
    - **whitelisting.[17]**
- **The risk assessment[18] for the obliged entity is not updated on an ongoing basis and the system of internal rules is not sufficiently adapted after changes.**

II. Prerequisites for effective and adequate AML transaction monitoring

i. Data and detection scenarios

In this area, emphasis is placed **in particular on the integrity and quality of input data** on all relevant transaction types, client behaviour, the nature of the business relationship[19] and ML/TF risk indicators for the assessment of potential risk exposure.

A prerequisite for AML monitoring is the **continuous, timely and quality evaluation of the effectiveness of individual detection scenarios, including the setting of relevant**

[15] Supervision practice shows that in the "main/overarching" SIR regulation there is usually only a very brief mention of AML monitoring, or no mention of AML monitoring at all. However, it is often not clear from this "main/overarching" SIR regulation whether such a thoroughly prepared methodological regulation on AML monitoring even exists. In view of this fact, it is advisable for obliged entities to mention a reference to the methodological regulation governing AML monitoring already in the "main/overarching" SIR regulation. Sensitive information, such as detailed procedures for setting detection scenarios, including the determination of detection limits ("thresholds"), is by nature part of the SIR, but it can nevertheless be expected that this information will only be available to a limited number of authorised persons (the "need to know" principle). In such cases, there may only be a reference in the framework AML regulation to a specific document, manual or methodology, which is available only to the AML/CFT department (with of course the possibility of review by internal audit, etc.).

[16] For example, an internal analytical document justifying the specific setting of limits in the context of the given obliged entity. An example of an imprudent approach is a situation where (i) the highest transaction by customers that are natural persons in the last year is CZK 1 000 000 and the limit of the scenario tracking unusual over-limit payments is set to CZK 5 000 000 (ii) the setting of limits does not take into account the specifics of the client segment, typically e.g. the difference between medium and large enterprises (generally termed “SME” and “LARGE CORP”) or directly the information provided by the client in the context of client due diligence, whether initial or ongoing.

[17] An explanation of the term "whitelist" and the “whitelisting” process is further elaborated in the "Alert Investigation Procedures, Whitelisting" section of this benchmark.

[18] Article 21a of the AML Act.

[19] For example, the nature of the business relationship, its duration, etc., within which the transactions are carried out.

detection parameters (e.g. transaction limits) to match the current risks in the context of risk assessment and RBA.[20]

In view of the above, the CNB considers the following approaches, for example, to be insufficiently prudent:

- **A relevant approach to data purity and integrity is not applied and therefore the data underlying the performance of AML monitoring lacks validity, accuracy or completeness. The result is a significant error rate in detecting client or transaction risk, albeit often within the framework of a sophisticated and costly solution.**

- **Data gaps arise when initial or periodic client due diligence is not performed at all or not performed to a sufficient extent to ensure a sufficient understanding of the AML risks associated with the client. These include financial institution clients and lawyer/notary clients when conducting custody of money through so-called custody accounts, where the obliged entities often lack knowledge of the structure of the client portfolio served by these clients, the quality of AML controls performed by them and their regulatory base in general.**

- **The setting of detection scenarios does not reflect the recommended standards, does not take into account the results of the actual implementation practice.**

- **The application of a single detection scenario(s) limit for all obliged entities within the group (i.e. also internationally active) means the local specificities of the given market/product/client groups etc. are not taken into account.**

ii. Internal transfers between accounts of the same client or between clients within the framework of a given obliged entity

In interpreting Article 4(1) of the AML Act, the CNB is inclined towards the interpretation practice whereby the term "transaction" means any disposal of a client's assets, meaning any type of interaction. This view is also supported by settled interpretive practice, e.g. "*The general term 'transaction' for the purposes of the AML Act refers to any interaction that could potentially lead to the legalization of proceeds. This therefore includes not only classical business transactions with a seller and a buyer and, for example, transfers between different accounts with the same owner are also considered as transactions for the purposes of this law. On the other hand, disposal of assets of the obliged entity does not meet the definition of a transaction - it must always be the disposal of the assets of another person. A transaction pursuant to the AML Act is not judged by the direction 'from a client' or 'to a client'; it is always a transaction - for example, in gambling both the bet and the winnings are considered transactions*."[21]. An obliged entity may also apply AML monitoring procedures to internal transfers between accounts of the same client or between accounts of different customers held by the same obliged entity. In this context, it will

[20] These processes must also be reconstructable in the sense of Article 18 of the AML Decree.

[21] Markéta Hlavinová, Viktor Kabeš, Jaroslava Pilíková. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (Act on Selected Measures against Legitimisation of Proceeds of Crime and Financing of Terrorism). Commentary. 3rd Issue. Prague: C.H.Beck, 2022, on Article 4 of the AML Act.

also proceed in accordance with an RBA and may therefore, on the basis of a prior assessment, identify only certain types of higher risk internal transfers and apply AML monitoring to those.[22]

In view of the above, the CNB therefore considers the approach to be insufficiently prudent, *inter alia*, in situations where an obliged entity does not monitor, or does not take into account, internal transfers between accounts of the same client or between accounts of different clients held by the same obliged entity [23] ("internal transfers") in the context of AML monitoring. As a result of this setup, these payments are virtually excluded from AML monitoring.

iii. Non-bank financial institutions in the position of a client of an obliged entity

According to the National Risk Assessment[24] , non-bank financial institutions (especially providers of payment and exchange services) are among the sectors highly vulnerable to ML/TF risk due to globalisation of trade and the development of digitalisation, and therefore pose an increased risk in the form of higher materialisation of individual ML/TF typologies. This risk must be accompanied by enhanced measures within the RBA that sufficiently mitigate it. For this reason, when entering into a business relationship with such clients and during the course of the relationship, it is necessary to apply enhanced client due diligence with respect to Article 9a(1) of the AML Act, respectively Article 9 of the AML Decree, in order to gain a deeper understanding of the given business relationship.

The main risk here is the execution of transactions by the client's clients, so we can talk about "nested" accounts. For obliged entities whose client is a financial institution, the risk is similar to that in correspondent banking. AML monitoring must therefore be able to effectively detect the risks associated with these specific types of customers - non-bank financial institutions.[25]

The obliged entity should not only rely on general information when performing due diligence for non-bank financial institution customers, but in particular obtain information sufficient to enable it to understand the nature and purpose of the business relationship with these customers, i.e. to understand the risk appetite of these customers, who are also obliged entities pursuant to the AML Act. In the case of this type of customers, the obliged entity should have information on how these customers manage the ML/TF risks of their own customers, i.e. information on:

[22] It can therefore be assumed that if no other risk factors are identified, it is not necessary to monitor e.g. a transfer between a current account and a savings/term account of the same client, cash pooling or an over-night account, etc. For example, transfers between the accounts of a person who simultaneously holds accounts as a natural person (consumer) and a natural person engaged in business can be considered as relevant situations.

[23] There may also be risk indicators, *inter alia*, in transfers within a single economically related group (ERG) or economically related group of persons (ERGP).

[24] See, for example, the document "*Report on the second round of the National Money Laundering and Terrorist Financing Risk Assessment Process*" published on the FAO website: https://www.financnianalytickyurad.cz/informace-o-druhem-kole-narodniho-hodnoceni-rizik.

[25] In this context, it is also appropriate to draw attention to the definition of the beneficial owner within the meaning of Article 4(4)(b) of the AML Act – the "beneficial owner of the transaction". For the purposes of this law, the beneficial owner is the natural person for whom the transaction is executed, while pursuant to Article 9(2)(b) of the AML Act, the obliged entity should know the identity of the beneficial owner, including the beneficial owner of the transaction. This is therefore a reminder of this legal obligation as one of the options within the framework of carrying out enhanced client due diligence in the event of increased risk or examination of a potentially suspicious transaction with regard to an individual/selected transaction or interrelated transactions.

- the quality of the AML rules and procedures in place[26],
- the business model (including in the context of whether it is expected to be feasible),
- the possible transactions it offers its customers (types of products/services),
- the structure of the portfolio of customers served by the non-bank financial institution in order to assess the relationship with the risky country of origin[27],
- the destinations from/to which payments will be made (in the context of possible ML/TF risky countries),
- the expected payment volumes and
- how it manages the risks associated with the implementation of international sanctions, etc.

As a result of executing client transactions, an obliged entity may, *inter alia*, be exposed to the risk of executing transactions that it would otherwise consider high-risk or directly unacceptable in the context of its risk appetite or RBA. AML monitoring should be able to monitor transactions in such a way that, in addition to checks against sanctions lists, it will use information obtained by the obliged entity through client due diligence, namely at least the structure or accumulation of transactions at client level (e.g. whether or not the transactions correspond to the declared volume/structure or are executed in relation to a country other than the one declared by the client, etc.). Another line of defence is close cooperation with the given client, respectively its staff responsible for the AML area.

In view of the above, the CNB therefore considers approaches to be insufficiently prudent, *inter alia*, in situations where the AML monitoring does not have specific detection scenarios that allow for timely and effective detection of suspicions in relation to customers of non-bank financial institutions, taking into account relevant risk factors and information from client due diligence (e.g. expected volumes/numbers of transactions vs. actual volumes/numbers).

iv. Investment instruments

client due diligence within the meaning of Article 9 of the AML Act includes all interactions (transactions) executed by the client. Therefore, regular client due diligence through AML monitoring also applies to the area of investment transactions. In practice, the CNB encounters situations where obliged entities have, in terms of AML monitoring, i.e. the "main" AML system, monitoring set up only for transactions on a client's current (payment) account. Therefore, individual transactions (interactions) carried out with so-called investment instruments within the meaning of Article 3 of Act No 256/2004 Coll., on capital market business, as amended (hereinafter the "CBM Act") (hereinafter "investment instruments") are no longer taken into account. As a rule, only incoming and outgoing payments (or final totals from individual transactions) with investment

[26] The information source may include, for example, the SIR (if voluntarily provided in full by the client), selected parts of the SIR (which will be relevant for the assessment of the measures applied by the client) or a summary of the measures applied by the client, suitably described by the client (possibly in the form of minutes from a meeting with the client at which this was discussed in the necessary detail). The so-called Wolfsberg AML Questionnaire is an appropriate form for supplementing client information, but should not be the only source of information, and the obliged entity should take other appropriate steps to obtain and verify the necessary information within the framework of client due diligence.

[27] This is to say, so that the obliged entity does not expose itself to the risk of executing intermediated payments for groups of customers with a relationship to selected risky countries, taking into account its own risk assessment (e.g. in the form of a measure that the client will not execute, through the obliged entity, transactions of its customers that have a relationship with a selected country of residence/stay or nationality).

instruments in relation to a client's current payment account are reviewed. This type of AML monitoring cannot in itself fulfil the main role of carrying out client due diligence to detect potentially suspicious trades. It is precisely the above scenario that is not able to detect suspicious activity in time and will not allow the obliged entity to prevent the execution of a suspicious transaction, but at most will only alert it to secondary manifestations of risk without the possibility to act in time.

The purpose of client due diligence in the context of a business relationship is to assess the business relationship as a whole, i.e. whether it makes sense, fits the risk profile of the client, and does not show signs of riskiness or suspiciousness. Input and output checks of funds with regard to their origin is of course important, but in the context of the above, it is necessary to take into account the monitoring of possible non-standard client behaviour within the business relationship as a whole, including within the framework of sub-indicators of riskiness during the execution of individual transactions/orders with investment instruments. Examples of riskiness and risk typologies can be found, for instance, in the documents listed below, particularly in the form of recognised standards and recommendations:

- Risk assessment by the bank,
- National risk assessment,
- Supranational risk assessment at European level,
- Recognised AML standards, in particular
  - FATF (2018), Guidance for a Risk-Based Approach for the Securities Sector,
  - EBA/GL/2021/02, in particular
    - Guideline 12: Sectoral guideline for wealth management,
    - Guideline 15: Sectoral guideline for investment firms,
    - Guideline 16: Sectoral guideline for providers of investment funds.

As a rule, obliged entities partially replace AML monitoring with specialised applications which, according to the obligations set out in the Market Abuse Regulation (MAR) regulatory framework, are primarily designed to detect other risks, e.g. “wash trade”[28], “painting the tape”[29] transactions, etc. These systems are therefore not intended to meet AML obligations and therefore by definition are not intended for ML/TF risk management and assessment.

Sufficient effectiveness of automated AML monitoring in the area of transactions with investment instruments is conditioned by its ability to compare transactions executed by the client in their entirety, i.e. both those on the current account and those related to investment instruments. Without such a functioning detection of potential suspiciousness, it is not possible to ensure the identification of all potential ML transactions or the identification of inconsistencies with the information obtained by the obliged entity. Specifically, the obliged entity has the following information available and evaluates it at client level, *inter alia* in the context of Article 7 of the AML Decree as information known to the obliged entity:

[28] This is the execution of transactions without actually changing the beneficial owner of the financial instrument. E.g. the CNB decision filed under No 2010/5287/570, relating to file No Sp/2009/188/573, dated 11/ 6/ 2010, in the case of party to the proceedings Patria Finance, a. s., or the CNB decision filed under No 2010/2786/110, relating to file No Sp/2009/165/573, dated 11/ 6/ 2010, in the case of party to the proceedings Raiffeisenbank, a. s., publicly available on the CNB's website.

[29] This is a situation in which an investor simultaneously sells and buys the same financial instruments, creating artificial activity.

AML area:

- client risk category,
- information obtained from initial and ongoing client due diligence[30], the client's assets (in particular the source of funds, the client's occupation/subject of business, their regular income), current and expected turnover on their "classic/current" account;

the area of provision of investment services, e.g. information in practice generally obtained in particular through the investment questionnaire[31] in the context of meeting selected capital market regulatory requirements for the purposes of:

- compliance with obligations when offering or recommending an investment instrument to a customer within the meaning of Article 12bb of the CBM Act and Article 15c of the CBM Act and others ("product governance" pursuant to MiFID II) and
- requesting information from customers pursuant to Article 15i of the CBM Act and Article 15h of the CBM Act in order to assess the adequacy and suitability of the investment service for the given customer (selected parts, see Annex 1)[32].

v. IS/IT prerequisites

IS/IT focuses on all AML IS/IT processes, in particular processes relating to change management and the development of software systems, security monitoring, security and operational incidents impacting AML functionality, access rights and information protection[33], information systems operation and business continuity. At banks, the IS/IT area is governed in particular by Article 11(2) and points 10 to 21 of Annex 6 to Decree No 163/2014 Coll. and also the EBA Guidelines on ICT and Security Risk Management.

The assumptions monitored are in particular:

- **A sufficient level of reconstructability of key parts of IS/IT processes - at least in the area of the definition and deployment of new versions/functionalities (including AML alert generation functionalities), operational steps such as disabling and enabling functionalities, access rights changes, security monitoring and security incidents, etc.**
- **A defined and effective process for change management and IS/IT development - all functional and non-functional requirements are clearly specified, tested and accepted by the person responsible for AML monitoring[34].**
- **Functional monitoring of important events of the systems used for AML monitoring, especially changes in access rights, changes in software versions, changes**

[30] In the sense of Article 9 and Article 9a of the AML Act and the requirements further elaborated in the AML Decree.

[31] Alternatively, by other appropriate means.

[32] The CNB also draws attention to other obligations associated with the completion of the investment questionnaire by the customer that are synergistic with compliance with AML requirements. This includes in particular the o bligation to (i) check the mutual consistency of the answers, (ii) check the reliability of the answers between questionnaires – this means, for example, detection of repeated purposeful completion of the investment questionnaire with the intention of achieving the desired investment profile, (iii) ensuring that the information is not manifestly out of date, inaccurate or incomplete - having a set period of time after which the customer must update the investment questionnaire, including notifying the customer that the information obtained needs to be updated if there is a material change in their actual situation.

[33] For example. DLP (Data Loss Prevention).

[34] Also referred to as the Business Owner.

in the execution of individual AML functionalities and AML procedures, as well as events defined as security incidents and the propagation of these incidents into the entire process of working with security incidents.

- **Defined and implemented architecture and integration of IS/IT systems in the area of AML monitoring that takes into account the requirements of business continuity management ("BCM") and is effective for meeting the requirements of AML monitoring, including with external systems such as external databases/registries. Typically, these are sanctions lists (both publicly available and commercial, which contain extended data sets) and other sources for verifying negative information or determining the riskiness of audited entities, e.g. CRIF, basic registers, BRKI (Bank Client Information Register), NRKI (Non-Bank Client Information Register), and the Solus interest association of legal persons.**
- **An implemented system for access permission management in IS/IT systems with need-to-know principles and the separation of incompatible roles.**
- **Effective outsourcing management in the case of outsourcing for IS/IT AML. Functional identification, monitoring and evaluation of outsourcing,[35] including understanding impacts in the event of a business continuity event (supplier failure) and data protection.**
- **Effectively implemented backups to meet the requirements of business continuity management, but also to support reconstructability, especially the possibility of reconstructing reported alerts at a defined point in time (this can also be solved in other ways, e.g. by appropriate archiving). Support for alert reconstructability refers not only to keeping a record of alert generation, but also to the history of alert processing.**
- **From a business continuity management perspective, IS/IT systems should be viewed as key systems in line with the connected surrounding systems such as online transaction systems and the data warehouse (DWH).**
- **Ensuring and maintaining data integrity for effective AML work. Where different languages and character sets are used, ensure compatible and efficient use of coding, code tables and transliteration of textual information so that information is not lost or confused, e.g. client names and addresses.**
- **Maintain up-to-date IS/IT system risk analysis for AML areas.**

III. Prerequisites for the process procedures area

i. Timeframes for alert generation and investigation

The purpose of Article 21(1) of the AML Act[36] is primarily to ensure that the procedures in place and applied are adequate and thus have the capacity and capability to fulfil their purpose, i.e. to mitigate and effectively prevent ML/TF risks. Thus, a system of internal rules

[35] Within the sense of EBA/GL/2019/02 - EBA Guidelines on outsourcing.

[36] Article 21(1) of the AML Act determines: *"The obliged entity introduces and applies adequate strategies and procedures of internal control and communication to mitigate and effectively manage risks of legitimisation of proceeds of crime and financing of terrorism identified in the risk assessment pursuant to Article 21a and to fulfil other obligations stipulated in this Act"*.

that does not have this fundamental characteristic and prerequisite will not be able to mitigate and effectively prevent ML/TF risks. Such risk prevention requires a pro-active approach, not a re-active approach.[37]

The basic prerequisite for AML monitoring is primarily the establishment and application of procedures for the timely detection, investigation and notification of suspicious transactions to the FAO pursuant to Article 18(1) of the AML Act so that the meaning and purpose of the AML Act is achieved in its entirety, i.e. so that funds can be secured in a timely manner if necessary.[38]

It is clear from the requirements set out in the AML Decree, and in particular in Article 17a, that the obliged entity must effectively monitor transactions so that it can detect and investigate any suspicions within a reasonable time. The AML Decree also implies that the obliged entity must implement automated searches for information, unless this is disproportionate to its size or the nature of its business (see Article 17(2) of the AML Decree). In the case of banks, given their size and complexity, no option other than processing through automated systems can be considered.

A key feature of such a system must be the appropriate setting of time limits for generating alerts and their subsequent investigation. The alert processing process will include all stages of its existence: generation, prioritization, investigation, closure. The investigation is then linked to the prioritization of alerts based on RBA. In general, the moment of initiation of the investigation of alerts as well as the length of the investigation of alerts should correspond to the risk level of the monitored typology, in conjunction with the risk of the given client/transaction. It should be noted that the time limit for investigating an alert starts when it is generated, not when it is "opened" (assigned to the appropriate staff member). An alert generated by a scenario tracking the daily or weekly transaction history assumes immediate processing, or at least within a few days. An alert generated by a scenario tracking a longer transaction history (weeks, months) or more complex conditions (e.g. cash-flow change, ERG/ERGP flows[39]) is expected to be processed within a month.

The time limit for processing an alert is influenced by a number of factors. An example is a situation where the client is asked to cooperate, e.g. to provide documents, but for objective reasons they cannot provide them immediately, e.g. they are on vacation/on a business trip abroad.[40] In such situations, the investigation time limit may be extended accordingly. These reasons may objectively make it difficult or even impossible to close the alert in time. If this is the case, the obstacles encountered to the timely processing of the alert must be included in the record of the investigation (closure), including a description of the steps taken to overcome them.

[37] All this is of course continuous while maintaining an RBA, which shows that some typologies are carried out before their implementation (ex-ante), e.g. checks of transactions against sanctions lists, and others after their implementation (ex-post), e.g. accumulation of cash transactions.

[38] The CNB also draws attention to the additional provision of Article 15 of the AML Act, which serves not only as a tool for the obliged entity to obtain the necessary information and supporting documents in the context of an alert investigation, but also in cases where there are doubts about the veracity of the information, where the notification pursuant to Article 18(1) of the AML Act is often implemented in combination with the application of the aforementioned Article 15 of the AML Act.

[39] There may also be risk indicators, *inter alia*, in transfers within a single economically related group (ERG) or economically related group of persons (ERGP).

[40] Other objective reasons may be situations such as (i) the illness of the client or the responsible employees of the legal entity (here, however, subject to a proper risk management function to ensure the expected level of substitutability); (ii) the client's answer raises further questions and the query needs to be repeated/clarified; (iii) the existence of public sources that can confirm the information about the transaction or obtained from the client, but can only be verified with a certain time delay; (iv) a delay caused by waiting for a response (especially from abroad).

In view of the above, the CNB considers the following approaches, for example, to be insufficiently prudent:

- **The generation of the alert itself takes place without distinction of situations (detection scenarios according to the monitored typologies) in so-called batches, usually after a number of weeks or up to 30 days. This is a situation where the condition of the detection scenario for generating the corresponding alert is already met, but the alert is generated and transmitted for verification in bulk within an individual batch.**
- **Extremely unreasonably long time limits are set for the actual investigation of individual alerts, usually in the order of tens to hundreds of days.[41] Such situations are created in particular in the cases of obliged entities that are part of an internationally operating group, where a system of so-called investigation centres (hubs) is created and to which the investigation itself is outsourced, with each additional investigation level (level) having a set time limit for the investigation. It is the sum of these sub-timelines that may ultimately create the premise for an unreasonably long investigation, i.e. the time from the actual execution of the transaction or sequence of transactions, as a result of which AML monitoring becomes to some extent a mere "paper exercise" that disregards the statutory purpose and intent of the measures.**

ii. Procedures for alert investigation, whitelisting

The simple and mechanical introduction of a system for reporting suspicious transactions, respectively the identification of alerts, or the inclusion of clients or individual client accounts on a "whitelist"[42] without taking into account the other follow-up activities of the obliged entity and at least the basic formalisation of the given procedures, results in a system that does not fulfil its function and can hardly constitute the fulfilment of the legal requirement and be an effective measure capable of managing ML/TF risks and contributing to the objective pursued by the AML Act, i.e. preventing money laundering and terrorist financing (cf. Article 1 of the AML Act).

An approach by an obliged entity based on an ad hoc subjective assessment of the situation cannot be considered sufficient. Such an approach, *inter alia*, creates an unreasonable burden on the AML system at the obliged entity, especially in view of the absence of a given methodology that would clearly set out the rules so that they could be adequately reviewed and enforced in relation to individual employees of the obliged entity. The aim and purpose is not to unduly increase the burden in the form of "bureaucratic" internal methodologies supposed to describe every possible situation in detail, but to define the basic procedures at least in basic terms. It is to be expected that each individual case (alert) has its own specifics. A certain degree of deviation is therefore to be expected, yet must be identifiable and verifiable in a reconstructable way. The rules and procedures for investigating alerts should also include a methodology for prioritising their investigation. This means a process that adequately takes an RBA into account,

[41] In practice, of course, a permissible deviation from the deadlines can be expected in justifiable situations - see the example given in the text above.

[42] I.e. an internal list of entities automatically excluded from monitoring.

where the investigation can reasonably be expected to start with higher-risk customers/transactions and end with the lowest-risk customers/transactions.[43]

The restriction of AML monitoring of entities or transactions, or "whitelisting", is generally permissible in the sense of simplified client due diligence pursuant to Article 13 of the AML Act.[44] In practice, from a technological point of view this is standard functionality of most systems. The use of whitelisting can be considered provided that the systemic measure used to manage AML/CFT is adequate and sufficiently robust to allow for individual and specific deviations from the set system (rather than blanket exclusion of groups of customers). However, such procedures must always be accompanied by both a methodology (see the previous part), justification in the context of risk management, and in particular by related control mechanisms for regular checking of the justification of the exemption.[45] These processes must also be reconstructable in the sense of Article 18 of the AML Decree. Therefore, if the management and control system of the controlled person in the area of AML/CFT meets such requirements, individual clients or client accounts can be whitelisted.

In view of the above, the CNB therefore considers, *inter alia*, that there is insufficient prudence where the SIR does not include formalised procedures for:

- **the investigation of individual alerts and the order in which they would be investigated taking into account the RBA;**
- **the inclusion of entities in exemptions from AML monitoring, or "whitelisting" (a mere setting within a given application/system is not sufficient), including proper justification and approval corresponding to the given risk, and regular review of justification for the application of simplified due diligence in the form of "whitelisting".**

iii. Alert closure

Each alert represents a potentially suspicious transaction that needs to be investigated, evaluated and closed. The closure then includes a statement to that effect, i.e. whether and why the suspiciousness of the transaction has been ruled out or not in the given case, and information on any further measures (e.g. refusal to execute the transaction, filing a suspicious trade report pursuant to the AML Act). The closure statement helps the obliged entity ensure the reconstructability of procedures and processes as required by the AML Act and the AML Decree[46].

In view of the above, the CNB therefore considers an approach to be insufficiently prudent where:

- **It is not possible to retrospectively reconstruct from the alert the reason and circumstances of the method of its resolution, including alerts closed without filing**

[43] However, even for the lowest-risk customers, the timeframes should be set in the context of the "Timeframes for alert generation and investigation" chapter of this supervision benchmark.

[44] Whitelisting within the limits of simplified client identification and due diligence must not be confused with exemption from client identification and due diligence within the meaning of Article 13a of the AML Act. Thus, pursuant to simplified client identification and due diligence, there is still an obligation to carry out due diligence to a precisely defined (limited) extent, taking into account the risks associated with the product and the client.

[45] Regular review should, *inter alia*, detect in a timely manner the presence of an ML/TF risk factor that would preclude retention on the whitelist.

[46] Article 16(3) of the AML Act and Article 18 of the AML Decree.

a suspicious transaction report or without applying Article 15 of the AML Act, i.e. refusal to execute the transaction.[47]

IV. AML monitoring using artificial intelligence (AI)

The CNB is aware of the trend towards the introduction of technologies that use artificial intelligence (AI) and the benefits arising from them. These are not only savings in terms of staff capacity required e.g. in the context of increasing alert volumes, but especially the potential benefit in terms of the quality of detection of individual suspicions[48], where it is possible to target more individual elements for each client. The CNB generally takes the position of technological neutrality and therefore does not oppose the introduction of AI systems in the area of AML.[49] The current use is quite broad, ranging from tools for initial client due diligence and the prioritization of individual alerts, which are still investigated by staff at the obliged entity, to fully automated investigation of alerts, which are subsequently verified. Like any technology, AI systems have their own pitfalls and risks that need to be detected and managed, with the appropriate measures developed.

In the case of the use of AI elements, the CNB considers the following to be a prudent approach:

- **Verification of the quality of the input, so-called learning data, on which the initial calibration (setup) of the AI will be performed.**[50]
- **A sufficient level of clarity and reconstructability of decision-making processes made by AI. The outcome of the process, e.g. the reasons for evaluating the alert, must be traceable. This is generally referred to as "self-explainable AI".**
- **The possibility of continuous calibration of the AI model. This is particularly the case when there is a relatively rapid change in circumstances/behaviour in a given segment.**[51]
- **Systems with AI elements are implemented by IT teams and in cooperation with the risk management department. AI systems need to include clear project documentation (in terms of deployment/implementation of the tool). Machine learning involves testing and continuous updating.**

[47] A typical shortcoming is simply stating "OK" without further explanation when an alert is closed.

[48] The CNB's findings in the context of supervision practice, discussions within the so-called "AML community" and, *inter alia*, statements from commercial entities, show that even a very well-tuned AML system based on rule-based scenarios shows an efficiency of about 10%. For example, "*Worldwide banks manually review millions of financial crime monitoring alerts per month with almost 95% of the alerts raised being 'non-suspicious'.*" https://home.kpmg/xx/en/home/services/advisory/risk-consulting/fighting-financial-crime/transaction-monitoring.html.

[49] In general, the AML Act and the AML Decree are technology-neutral in nature, including in relation to AML monitoring.

[50] This is, for example, the issue of the so-called "data anchors" that AI creates during the learning process. Example of bad calibration (learning data) - the system should have recognized a wolf from the animal photo files. The system showed a 98% success rate. It was later discovered that it always recognized the wolf because there was snow in the background of the picture with the wolf. When the snow was removed, the success rate for wolf recognition dropped to 50%.

[51] An example is the onset of a pandemic, which results in society-wide changes, including changes in the behaviour of individual customers. Examples include increased cash withdrawals (onset of pandemic, insecurity), increased payments at e-shops/use of credit cards (homeoffice work, merchants demanding only contactless payments, etc.). An opposite example could be a situation in which a company reported the same cash sales during the lock-down period.

- **The issue of so-called "program bias" in the system's decision-making is addressed. One assumption is the mitigation of risk arising from the circumstance that AI systems learn from a dataset on which they were 'trained' - depending on how this compilation was made, there is the possibility that the dataset will reflect assumptions or biases. These prejudices can then influence the system's decision-making and lead to unjustified discrimination.**
- **Maintain maximum system transparency. It is necessary that a system user is able to explain the rules of operation of the AI and that these can be continuously verified for correctness of settings or operation - it must not be a "black box".**

Conclusion

In the context of the above assumptions, the CNB expects an obliged entity to adopt AML monitoring procedures and measures that will ensure effective prevention of money laundering and terrorist financing, including effective detection of potentially suspicious transactions that will not ultimately expose it to the risk of failing to report suspicious transactions in a timely manner.

Annex 1 - Selected parts of MiFID II requirements for the purpose of: (i) product governance and (ii) suitability assessment

Suitability	Product governance
Article 54+ Article 55 *Regulation 2017/565* + *ESMA Guidelines*	*Article 18 of the* *ESMA Guidelines*
	The **type of customers** for whom the product is intended: The business should define the type of customer for which the product is intended. This definition should be made on the basis of the categorisation of customers pursuant to MiFID II as 'retail', 'professional' and 'counterparty'.
Investment **knowledge**: the types of services, transactions and financial instruments the customer is familiar with.	**Knowledge and experience**: The business should define the knowledge that target customers should have about each element, such as: relevant product type, product features or knowledge in topic-related areas that help to understand the product. For example, for structured products with a complex return profile, businesses could define that target investors should know how this type of product works and should know the likely outcomes of the product. In terms of experience, the business could describe the range of practical experience of the target customers with elements such as: relevant product type, relevant product features or experience in thematically related areas. For example, a business could define a period of time for which customers should be active in the financial markets. In some cases, knowledge and experience may be interdependent (i.e. an investor with limited or no experience could be an eligible target customer if their lack of experience is counterbalanced by extensive knowledge).
Investment **experience**: the nature, volume and frequency of transactions in financial instruments that the customer makes and the length of time for which they are made.	
Education and occupation or relevant former occupation of the customer or potential customer.	
Financial background, including loss-absorbing capacity: information on the financial situation of a customer or potential customer will include information on the source and amount of their regular income, their assets, including liquid assets, investments and real estate, and their regular financial commitments.	**Financial situation with a focus on the ability to bear losses**: The business should define in percentage terms the losses that target customers should be able and willing to bear (for example, from minimal losses to total loss) and should define whether there are any additional payment obligations that may exceed the amount invested (for example, calls for additional payment). This can also be expressed as the maximum proportion of assets that should be invested.
Investment objectives, including risk tolerance: information on the investment objectives of the customer or potential customer includes information on the length of time the customer wishes to hold the investment, their risk preferences, their risk profile and their investment objectives.	**Risk tolerance and compatibility of the product's risk/reward ratio with the target market:** The business should define the general attitude that target customers should have towards the risks of the investment. Basic attitudes towards risk should be categorised (e.g. 'risk-oriented or speculative', 'balanced', 'conservative') and clearly described. As different businesses in the chain may have different approaches to defining risk, the business should clearly set out the criteria that must be met when categorising a customer in this way. In complying with this requirement, businesses should use the risk indicator set out in the Packaged retail and insurance-based investment products (PRIIPs) Regulation or the UCITS Directive, as appropriate.
	Customer goals and needs: The business should define the investment objectives and needs of the target customers that the product is intended to meet, including the broader financial objectives of the target customers and the overall investment strategy followed. For example, the expected investment horizon (the number of years the investment is to be held) could be mentioned. These objectives can be "fine-tuned" by defining specific aspects of the investment and the expectations of the target customers. The specific customer goals and needs the product is intended to meet can range from the specific to the more general. For example, a product may be designed to meet the needs of a particular age group, to be tax efficient based on the customers' country of tax residence, or be designed with specific product features to potentially meet certain investment objectives such as "currency protection", "green investments", "ethical investments", etc.